ID: 1301138
Sample Name: file.exe
Cookbook: default.jbs
Time: 16:49:14
Date: 31/08/2023
Version: 38.0.0 Beryl

Table of Contents

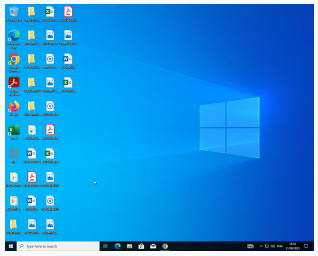
Windows Analysis Report

file.exe

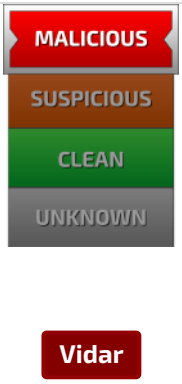
Overview

General Information

Sample Name:	file.exe
Analysis ID:	1301138
MD5:	bf81661814944..
SHA1:	7e3235d7ce69…
SHA256:	a524fce6eb4ee..
Tags:	exe
Infos:	



Detection



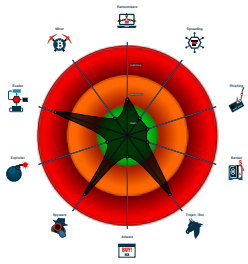
Vidar

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Yara detected Vidar stealer
- Detected unpacking (changes PE se…
- Tries to steal Crypto Currency Walle…
- Tries to harvest and steal Putty / W…
- Uses known network protocols on n…
- Searches for specific processes (lik…
- Machine Learning detection for sam…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 7912 cmdline: C:\Users\user\Desktop\file.exe MD5: BF81661814944B92DA689F1C461EF908)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Vidar	Vidar is a forked malware based on Arkei. It seems this stealer is one of the first that is grabbing information on 2FA Software and Tor Browser.	No Attribution	http://https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-1-(-Unpacking-)/https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-2/https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/vidar-stealer-h-and-m-campaignhttps://0xtoxin.github.io/malware%20analysis/Vidar-Stealer-Campaign/https://asec.ahnlab.com/en/22932/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar

Malware Configuration

Threatname: Vidar

```
{
  "C2 url": [
    "https://steamcommunity.com/profiles/76561199545993403",
    "https://t.me/vogogor"
  ],
  "Botnet": "b2ced91faf30889899f34458f95b8e93",
  "Version": "5.4"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.3698889782.0000000004100000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000001.00000002.3698889782.0000000004100000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000001.00000002.3696575131.000000000252E000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.3698810477.0000000004090000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x778:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000001.00000002.3693314502.0000000000400000.00000040.00000001.01000000.00000003.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.file.exe.4100e67.1.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.2.file.exe.4100e67.1.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.2.file.exe.400000.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.3.file.exe.4160000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
1.2.file.exe.400000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance

Detected unpacking (overwrites its own PE header)

Networking

Uses known network protocols on non-standard ports

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

HIPS / PFW / Operating System Protection Evasion

Searches for specific processes (likely to inject)

Stealing of Sensitive Information

Yara detected Vidar stealer

Tries to steal Crypto Currency Wallets

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Found many strings related to Crypto-Wallets (likely being stolen)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

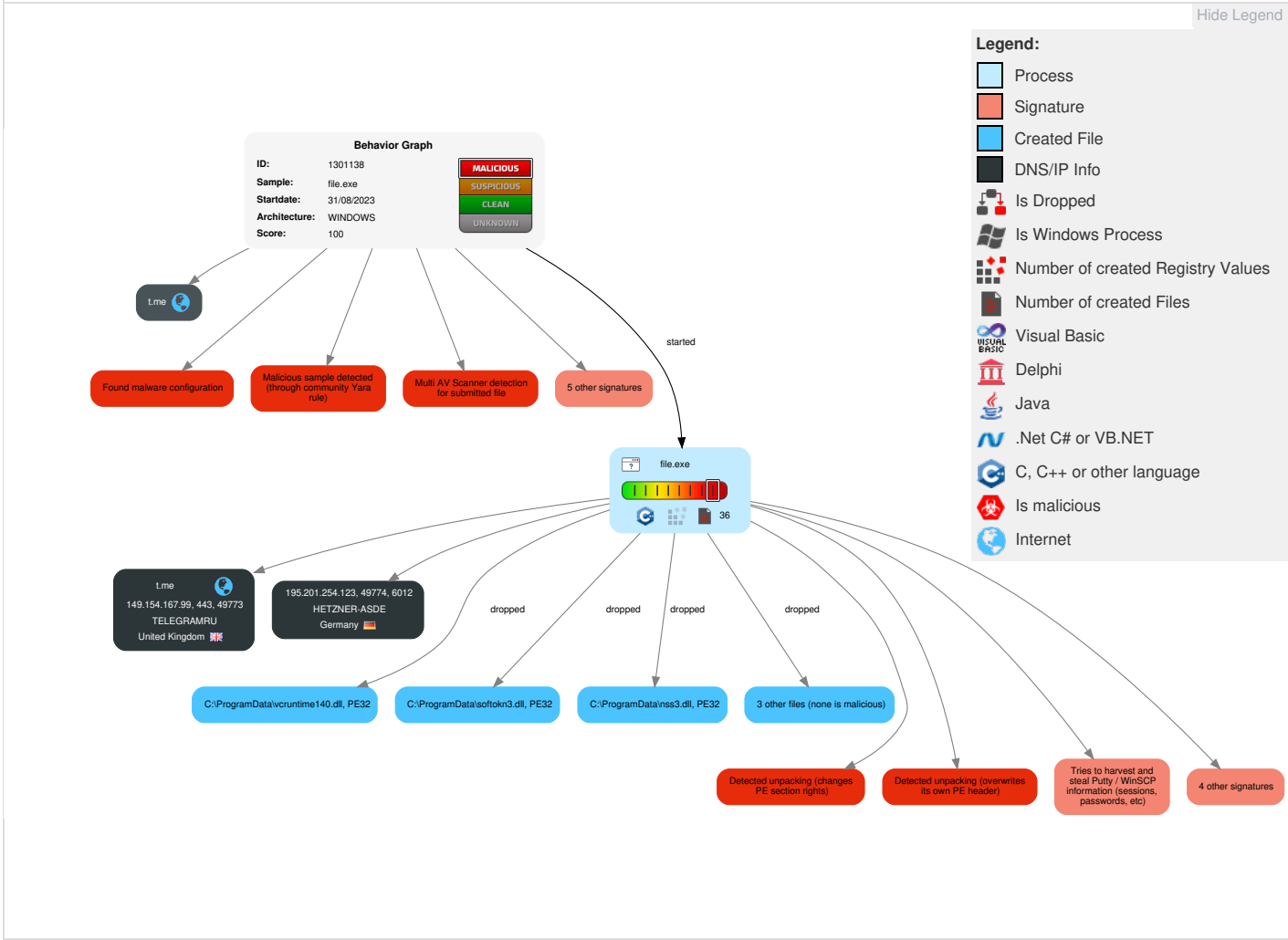
Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	Path Interception	1 Process Injection	1 Process Injection	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	4 1 Security Software Discovery	Remote Desktop Protocol	3 Data from Local System	Exfiltration Over Bluetooth	1 1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	2 Native API	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	1 2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 2 Software Packing	NTDS	1 Account Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	4 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 System Owner/User Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 5 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	3 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	3 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

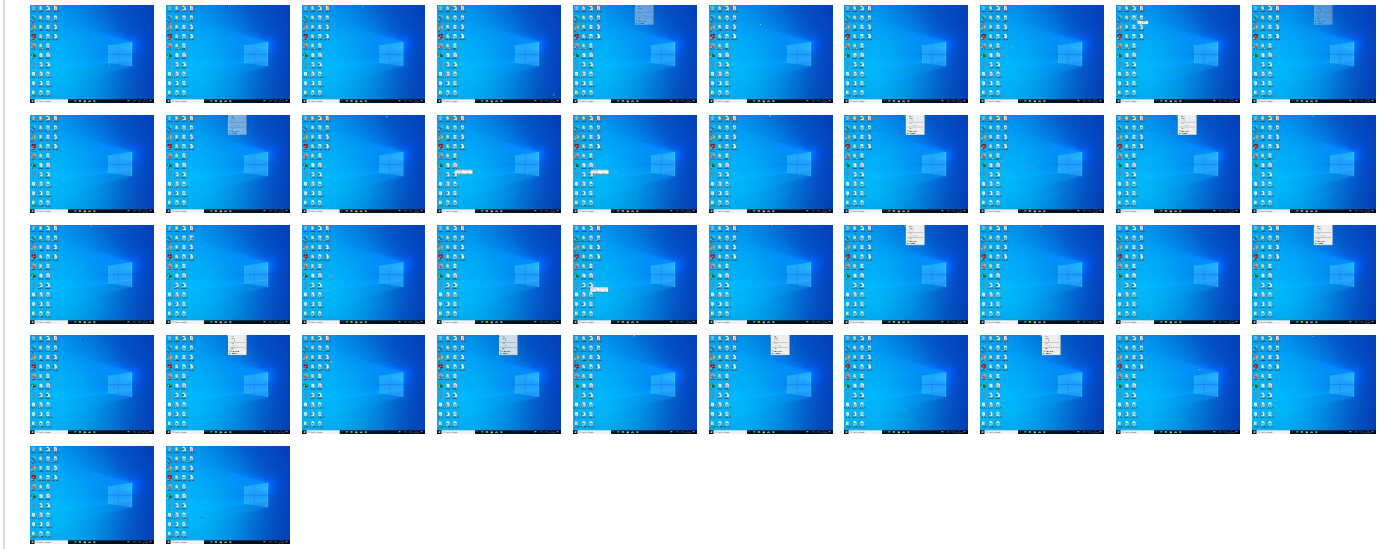
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
file.exe	66%	ReversingLabs	Win32.Ransomware.StopCrypt	
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\freebl3.dll	0%	ReversingLabs		
C:\ProgramData\mozglue.dll	0%	ReversingLabs		
C:\ProgramData\msvcp140.dll	0%	ReversingLabs		
C:\ProgramData\nss3.dll	0%	ReversingLabs		
C:\ProgramData\softokn3.dll	0%	ReversingLabs		
C:\ProgramData\vcruntime140.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://mozilla.org0/	0%	URL Reputation	safe	
http://195.201.254.123:6012/sp1.zip	0%	Avira URL Cloud	safe	
http://195.201.254.123:6012/sCodecs.dlls	0%	Avira URL Cloud	safe	
http://195.201.254.123:6012/m	0%	Avira URL Cloud	safe	
http://195.201.254.123:6012/b2ced91faf30889899f34458f95b8e93	0%	Avira URL Cloud	safe	
http://195.201.254.123:6012/Mu	0%	Avira URL Cloud	safe	
http://195.201.254.123:6012/0	0%	Avira URL Cloud	safe	
http://195.201.254.123:6012/b2ced91faf30889899f34458f95b8e93k	0%	Avira URL Cloud	safe	
http://195.201.254.123:6012/sp1.zipn)	0%	Avira URL Cloud	safe	
http://195.201.254.123:6012/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
t.me	149.154.167.99	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://195.201.254.123:6012/sp1.zip	false	• Avira URL Cloud: safe	unknown
http://195.201.254.123:6012/b2ced91faf30889899f34458f95b8e93	false	• Avira URL Cloud: safe	unknown
http://https://steamcommunity.com/profiles/76561199545993403	false		high
http://195.201.254.123:6012/	false	• Avira URL Cloud: safe	unknown
http://https://t.me/vogogor	false		high

URLs from Memory and Binaries

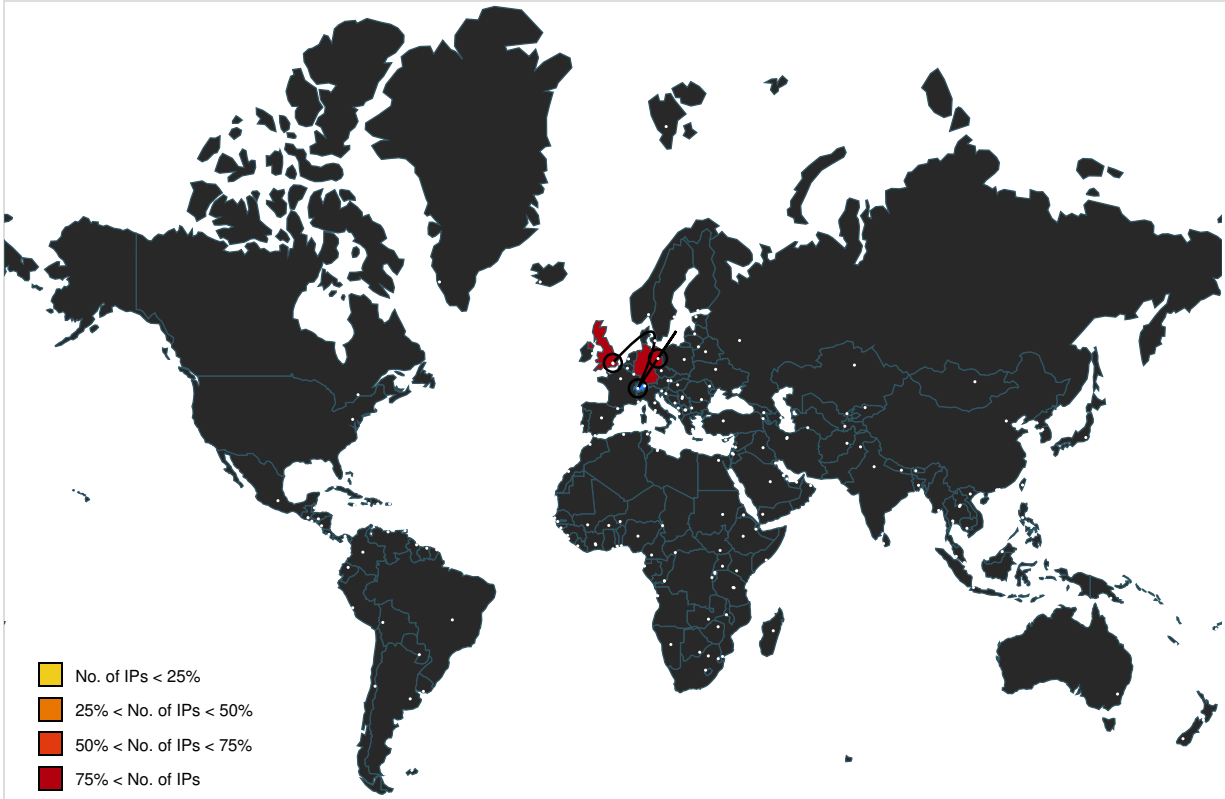
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	00440746450577075373182215.1.dr, 3770799051060493265496613 3.1.dr, 60379239670748708072323449.1.dr, 592426706128316606241 68672.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t.me/	file.exe, 00000001.00000002.3721084273.0 000000004A5F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/vogogorx	file.exe, 00000001.00000002.3721084273.0 000000004A5F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	6037923967074870807232344 9.1.dr, 5924267061283166062416867 2.1.dr	false		high
http://https://t.me/vogogorv	file.exe, 00000001.00000002.3707864447.0 00000000464E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://195.201.254.123:6012/Mu	file.exe, 00000001.00000002.3701045776.0 0000000043F6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://195.201.254.123:6012/sCodecs.dlls	file.exe, 00000001.00000002.3723888260.0 000000004C90000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	0044074645057707537318221 5.1.dr, 3770799051060493265496613 3.1.dr, 6037923967074870807232344 9.1.dr, 5924267061283166062416867 2.1.dr	false		high
http://https://www.google.com/chrome/thank-you.html?statcb=1&installdataindex=empty&defaultbrowser=0	file.exe, 00000001.00000002.3730149645.0 00000001198E000.00000004.00020000.00000000.sdmp, file.exe, 00000001.00000003.1564532439.0000000010EB7000.00000004.00000020.00020000.00000000.sdmp, 3834501395947130684624542.1.dr, 9370236560048579205996392 7.1.dr	false		high
http://195.201.254.123:6012/0	file.exe, 00000001.00000002.3698626677.0 000000002606000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.autoitscript.com/files/autoit3/autoit-v3-setup.zipQ	3056267190738054327250738 8.1.dr, 0581704168837594229622676 4.1.dr	false		high
http://https://sdlc-esd.oracle.com/ESD6/JSCDL/jdk/8u321-b07/df5ad55fdd604472a86a45a217032c7d/jre-8u321-wind	3056267190738054327250738 8.1.dr, 0581704168837594229622676 4.1.dr	false		high
http://https://t.me/vogogorracvotsp1.zipMozilla/5.0	file.exe, 00000001.00000002.3698889782.0 000000004100000.00000040.00001000.00020000.00000000.sdmp, file.exe, 00000001.00000002.3693314502.0000000000400000.00000040.00000001.01000000.00000003.sdmp, file.exe, 00000001.00000003.1481373645.0000000004160000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.google.com/chrome/	9370236560048579205996392 7.1.dr	false		high
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	0044074645057707537318221 5.1.dr, 3770799051060493265496613 3.1.dr, 6037923967074870807232344 9.1.dr, 5924267061283166062416867 2.1.dr	false		high
http://https://t.me/vogogorL	file.exe, 00000001.00000002.3707864447.0 00000000464E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fq%3Dmicrosoft%26oq%3Dmic	0581704168837594229622676 4.1.dr	false		high
http://https://www.google.com/search?q=test&oq=test&aqs=chrome..69i57j0i131i433i512j0i512j0i131i433i512l2j0	0581704168837594229622676 4.1.dr	false		high
http://https://stubdownloader.services.mozilla.com/?attribution_code=c291cmNlPXd3dy5nb29nbGUuY29tJm1lZGl1bT	3056267190738054327250738 8.1.dr, 0581704168837594229622676 4.1.dr	false		high
http://https://steamcommunity.com/profiles/76561199545993403update.zip	file.exe, 00000001.00000002.3698889782.0 000000004100000.00000040.00001000.00020000.00000000.sdmp, file.exe, 00000001.00000002.3693314502.0000000000400000.00000040.00000001.01000000.00000003.sdmp, file.exe, 00000001.00000003.1481373645.0000000004160000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.google.com/https://www.google.com/chrome/Thu	file.exe, 00000001.00000003.1565422518.0 000000010EB7000.00000004.00000020.00020000.00000000.sdmp, 3834501395947130684624542.1.dr, 9370236560048579205996392 7.1.dr	false		high
http://https://www.google.com/search?q=microsoft&oq=microsoft&gs_lcrp=EgZjaHJvbWUqEAgAEAAYgwEY4wIYsQMYgAQyE	0581704168837594229622676 4.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sqlite.org/copyright.html.	file.exe, 00000001.00000002.3730836231.0 000000061ED3000.00000004.00001000.000200 00.00000000.sdmp, file.exe, 00000001.000 00002.3729067726.00000000108F7000.000000 04.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/search?q=microsoft&sourceid=chrome&ie=UTF-8microsoft	05817041688375942296226764.1.dr	false		high
http://195.201.254.123:6012/b2ced91faf30889899f34458f95b8e93k	file.exe, 00000001.00000002.3707864447.0 000000004670000.00000004.00000020.000200 00.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mozilla.com/en-US/blocklist/	mozglue.dll.1.dr	false		high
http://https://aka.ms/vs/17/release/vc_redist.x64.exeD	30562671907380543272507388.1.dr, 0581704 1688375942296226764.1.dr	false		high
http://https://mozilla.org0/	file.exe, 00000001.00000002.3729241460.0 000000010A10000.00000004.00000020.000200 00.00000000.sdmp, softokn3.dll.1.dr, mozglue.dll.1.dr, nss3.dll.1.dr, freebl3.dll.1.dr	false	• URL Reputation: safe	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	00440746450577075373182215.1.dr, 5924267 0612831660624168672.1.dr	false		high
http://https://javadl.oracle.com/webapps/download/AutoDL?BundleId=245807_df5ad55fdd604472a86a45a217032c7dM	30562671907380543272507388.1.dr, 0581704 1688375942296226764.1.dr	false		high
http://195.201.254.123:6012/sp1.zipn)	file.exe, 00000001.00000002.3698626677.0 0000000025E1000.00000004.00000020.000200 00.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	60379239670748708072323449.1.dr, 5924267 0612831660624168672.1.dr	false		high
http://https://www.autoitscript.com/cgi-bin/getfile.pl?autoit3/autoit-v3-setup.zip	30562671907380543272507388.1.dr, 0581704 1688375942296226764.1.dr	false		high
http://https://www.google.com/search?q=test&sourceid=chrome&ie=UTF-8test	30562671907380543272507388.1.dr, 0581704 1688375942296226764.1.dr	false		high
http://195.201.254.123:6012/m	file.exe, 00000001.00000002.3698626677.0 000000002606000.00000004.00000020.000200 00.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.ecosia.org/newtab/	37707990510604932654966133.1.dr, 6037923 967074870807232 3449.1.dr	false		high
http://https://dl.google.com/tag/s/appguid%3D%7B8A69D345-D564-463C-AFF1-A69D9E530F96%7D%26iid%3D%7B27E81B29	38345013959471306846242542.1.dr, 9370236 5600485792059963927.1.dr	false		high
http://https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-br	file.exe, 00000001.00000003.1509460859.0 00000001103E000.00000004.00000020.000200 00.00000000.sdmp, file.exe, 00000001.000 00002.3729784367.000000001116C000.000000 04.00000020.00020000.00000000.sdmp, 7736 4074545019038892817732.1.dr	false		high
http://https://support.mozilla.org/products/firefox	file.exe, 00000001.00000002.3729784367.0 00000001116C000.00000004.00000020.000200 00.00000000.sdmp	false		high
http://https://www.google.com/chrome/thank-you.html?statcb=1&installdataindex=empty&defaultbrowser=0Google	937023656004857920599639 27.1.dr	false		high
http://https://www.google.com/favicon.ico	60379239670748708072323449.1.dr	false		high
http://https://ac.ecosia.org/autocomplete?q=	60379239670748708072323449.1.dr	false		high
http://https://www.autoitscript.com/site/autoit/downloads/	file.exe, 00000001.00000003.1536347021.0 000000010EB7000.00000004.00000020.000200 00.00000000.sdmp, file.exe, 00000001.000 00002.3729994076.000000001157C000.000000 04.00000020.00020000.00000000.sdmp, 3056 267190738054327250738 8.1.dr, 05817041688 375942296226764.1.dr	false		high
http://https://www.google.com/chrome/Google	937023656004857920599639 27.1.dr	false		high
http://https://www.autoitscript.com/site/autoit/downloads/https://www.autoitscript.com/site/Sun	05817041688375942296226764.1.dr	false		high
http://https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fq%3Dtest%26oq%3Dtest%26a	05817041688375942296226764.1.dr	false		high
http://https://support.mozilla.org	77364074545019038892817732.1.dr	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	60379239670748708072323449.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/search?q=microsoft&sourceid=chrome&ie=UTF-8microsoftt	30562671907380543272507388.1.dr, 0581704168837594229622676 4.1.dr	false		high
http://https://support.mozilla.org/products/firefoxgro.allizom.troppus.	file.exe, 00000001.00000003.1509460859.000000001103E000.00000004.00000020.00020000.00000000.sdmp, 7736407454501903889281 7732.1.dr	false		high
http://https://cdn.stubdownloader.services.mozilla.com/builds/firefox-stub/en-US/win/4b14f052f39ceffb32abd8	30562671907380543272507388.1.dr, 0581704168837594229622676 4.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.99	t.me	United Kingdom		62041	TELEGRAMRU	false
195.201.254.123	unknown	Germany		24940	HETZNER-ASDE	false

General Information

Joe Sandbox Version:	38.0.0 Beryl
Analysis ID:	1301138
Start date and time:	2023-08-31 16:49:14 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10, Office Professional Plus 2016, Chrome 115, Firefox 115, Adobe Reader 23, Java 8 Update 381
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	file.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@1/22@1/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.4% (good quality ratio 1.1%) • Quality average: 51.5% • Quality standard deviation: 39.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, RuntimeBroker.exe, WMIADAP.exe, SIHClient.exe, SgrmBroker.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): cp501.prod.do.dsp.mp.microsoft.com, www.bing.com, geover.prod.do.dsp.mp.microsoft.com, client.wns.windows.com, fs.microsoft.com, slscr.update.microsoft.com, login.live.com, disc501.prod.do.dsp.mp.microsoft.com, array510.prod.do.dsp.mp.microsoft.com, ctldl.windowsupdate.com, fe3cr.delivery.mp.microsoft.com
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: file.exe

Simulations

Behavior and APIs

Time	Type	Description
16:50:56	API Interceptor	1x Sleep call for process: file.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\00440746450577075373182215

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3034000, page size 2048, file counter 6, database pages 53, cookie 0x22, schema 4, UTF-8, version-valid-for 6
Category:	dropped
Size (bytes):	110592
Entropy (8bit):	1.103154063201814
Encrypted:	false
SSDEEP:	192:GLKnLLJFXH92HbG9mTjwnWxDnP1r6TVum:CKXJF392OnsDnRyVum
MD5:	A7888E78317DB24AF1E57A1E76360A05
SHA1:	350BC0A9A062F2290D8E41D17CACE4B49833918C
SHA-256:	34553CD7235802E2D02A4B1614D4C468E220377771CC7CB1A3F4D89580158534
SHA-512:	B705C5B67A2B294EB2951D19863F1FA729CE560C00378509D52AFDCBFAB824D754E32B013AB1318C17E9BC66B584471BFC01362A2BD3002AB3C388336ECD03E A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....5....."..... K.....*..... ....

C:\ProgramData\05817041688375942296226764

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3041002, file counter 9, database pages 43, 1st free page 42, free pages 2, cookie 0x3f, schema 4, UTF-8, version-valid-for 9
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.1974772984231898
Encrypted:	false
SSDEEP:	768:i99HO2V93qjTU6SwO3mFthT1RTt61Y6UTD6rT19TC61276:i9vj6SwO3mFLT/TEzUTGrT7Tr1
MD5:	C6DC96A2E44E44C2935599EED3825093
SHA1:	37BD985F5AF5FBB1D78B4E32E9C8A3965296EE01
SHA-256:	44E5DFBBF36F186126F7AAA8DF09475D5A5C259F3918DCBED8E29A918DBB479C
SHA-512:	3236C33C7447BF74DDE20B12A41DCCF2D2DBFE30557D8369F3EDE0DC9130B3FE3F4ABB055855EB97E150DE3AF0F2131E7DD9BCD760DA68F5BBEE55FDFAB2 BAD4
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....+...*.....?.....f..... ....

C:\ProgramData\22428703343438507335441715

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, user version 12, last written using SQLite version 3037002, page size 32768, writer version 2, read version 2, file counter 3, database pages 3, cook ie 0x1, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	524288
Entropy (8bit):	0.032592440528298426
Encrypted:	false
SSDEEP:	24:DQAVzff32mNVpP965Ra8KN0MG/lEKDIH5UMJKvuVKuQctWHB6Ox:DQM9rhvWTJcUOHhF
MD5:	16E2B74FCB83C62360F0E1A06C722FB8
SHA1:	D1450274E08468E3A650BE5D9E1086968CA234FE
SHA-256:	5FE70426BBB99C3D03AB2C33429FFFCE6F95B41073F45C918534A126708CE516
SHA-512:	AA47F896592296441ED00BC3C16737026E1FBA508D5EE038C1C2E535165ED14AFC8FBF49509FBDC87AFD1BF9005B2DDE7A5442173888767D3A8B05A33459302
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....WJ.....}..}..... ....

C:\ProgramData\22428703343438507335441715-shm

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.017262956703125623
Encrypted:	false
SSDEEP:	3:G8lQs2TSlElQs2TtPRp//:G0QjSaQjrpX
MD5:	B7C14EC6110FA820CA6B65F5AEC85911
SHA1:	608EEB7488042453C9CA40F7E1398FC1A270F3F4
SHA-256:	FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB
SHA-512:	D8D75760F29B1E27AC9430BC4F4FFCEC39F1590BE5AEF2BFB5A535850302E067C288EF59CF3B2C5751009A22A6957733F9F80FA18F2B0D33D90C068A3F08F3B
Malicious:	false
Preview:	..-.....8...5.....-.....8...5.....

C:\ProgramData\30562671907380543272507388

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3041002, file counter 9, database pages 43, 1st free page 42, free pages 2, cookie 0x3f, schema 4, UTF-8, version-valid-for 9
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.1974772984231898
Encrypted:	false
SSDEEP:	768:i99HO2V93qjTU6SwO3mFthT1RTt61Y6UTD6rT19TC61276:i9vj6SwO3mFLT/TEzUTGrT7Tr1
MD5:	C6DC96A2E44E44C2935599EED3825093
SHA1:	37BD985F5AF5FBB1D78B4E32E9C8A3965296EE01
SHA-256:	44E5DFBBF36F186126F7AAA8DF09475D5A5C259F3918DCBED8E29A918DBB479C
SHA-512:	3236C33C7447BF74DDE20B12A41DCCF2D2DBFE30557D8369F3EDE0DC9130B3FE3F4ABB055855EB97E150DE3AF0F2131E7DD9BCD760DA68F5BBEE55FDFAB2BAD4
Malicious:	false
Preview:	SQLite format 3.....@ .....+...*.....?.....f.....

C:\ProgramData\35746121865178509047716708

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3034000, page size 2048, file counter 2, database pages 23, cookie 0xd, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7621373211432615
Encrypted:	false
SSDEEP:	48:53oBA+IIH2KLk8s8LKvUf9KVyJ7h/ICVEq8MX0D0HSFlNUKxK3f3lGNxotkGY:tYMKLyeymwxCn8MZyFldK3PlGNxotk
MD5:	6F5AAE47EB95404578CBC4AB886A1214
SHA1:	3AC370895A57F1DB1BC96B8BB81BB70DD6872BD5
SHA-256:	376C5828CE6104EC467A4F29E30151DED0FCDF7BF14239E2D97661061A226E00
SHA-512:	891CA3343DEBEB3CE7419CBE4D021DE59A02986F0EADA64E07E72B40D7515F2D962B90A2C01FB0D997275C1382BE2E1ABBF517DF3AFA530B02894C4160530B02
Malicious:	false
Preview:	SQLite format 3.....@ .....K.....

C:\ProgramData\37707990510604932654966133

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3041002, page size 2048, file counter 7, database pages 57, cookie 0x30, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	118784

Entropy (8bit):	1.202433056168029
Encrypted:	false
SSDEEP:	192:8mEcY8dBLH95TkVb39nJnieheVuKht6jTAs5u:8JcYiBz9EJnieheVuK7u0s8
MD5:	1D1D49B9691A566CD1923A0929480A3D
SHA1:	93976FCE24A3C1F8ECED9E2516BD775215AA5834
SHA-256:	FE23175F9F3E20359907D9A10FC3A7210F4D60096EA38A1AD2CBC86AAE015ABC
SHA-512:	3B6B31D164CB51C9B6740D82BEA21EB66E30B7E7AF0672B0AB1A7C860FB9FA81D7FFC651BE93BDD5AC76AE4191C6C3402F835F8D6FA807ECF005EA5CE6A856D3
Malicious:	false
Preview:	SQLite format 3.....@ .....9.....0.....f.....6.....

C:\ProgramData\383450139594713068462425 42

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3034000, file counter 5, database pages 29, cookie 0x16, schema 4, UTF-8, version-valid-for 5
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.8330799750773747
Encrypted:	false
SSDEEP:	192:5A6DwbHq260V37/+bDo3irhnydVj3XBBE3uEUM:5AvHMi37wU3iVy/BBE3ulM
MD5:	5B8792E38274088A888A41F4AE3709EB
SHA1:	102DCDBAF4DDB1E3E37859EC1EDD1C788D75AF11
SHA-256:	090F856C8BD32598418336550AE669A11D44B9498FD7DDA794460D8B08F55515
SHA-512:	5B57092076CAFDECE39018B47DC6899F4D4F53E3EFD710AB471B00E0DE477E26868145C389E6841A5AC7840F9968FABF97AA5459520F51C6EA36EC71C8E089C5
Malicious:	false
Preview:	SQLite format 3.....@ .....K.....

C:\ProgramData\418543900811584738426950 81

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3041002, page size 2048, file counter 2, database pages 25, cookie 0x10, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	53248
Entropy (8bit):	0.8118330999829729
Encrypted:	false
SSDEEP:	96:/WtihQKLPeymwHCn8MouOFlWSHRmvlGNxut2ke:/Y0LHG7qHslGNx3
MD5:	066E1A9804AD57076FA92B00D773CDC0
SHA1:	FC9C1E0F8D28F9B69150B5E462A8F9E4504B4578
SHA-256:	64F215F7997D7B368586988808CC8BC9A9DCF8CED6E9EB648917BC2FDA453CFD
SHA-512:	71162B591EAE3C1A07F7F15079053560E5CD232A8A5BF300F3BD5A31BF1BA69B7158848EC69F4F1BDE1516B1FF161A6341A1C016DE81795EDB1E35512BF618D7
Malicious:	false
Preview:	SQLite format 3.....@ .....f.....

C:\ProgramData\527660143035014 64703169876

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3034000, file counter 11, database pages 8, 1st free page 8, free pages 1, cookie 0x4, schema 4, UTF-8, version-valid-for 11
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	2.7230981948383226
Encrypted:	false
SSDEEP:	96:z7NwCzfH7s05cCsdsYMu05V+k9w0kI0kIFR8Au7k0Z6nu0cfG0GC+6isqlkus40w:HuyHjgMJuY6u0JRlWNNBDqD/
MD5:	56A0DB5DFC56C74D2657D5C579DE93CE

SHA1:	ACC535D924463C4710805BAF65188169684EE3E6
SHA-256:	52C44B402FAD0B7D0AE2F90007D170CB24D3D327E49061267444A119926F7DFA
SHA-512:	75321A07514D68F515C78C5395215BF00C5DFF5060F9C33FCD30D66EBE146245AA6DFFD8BCAE8747AD09D7B34630DA723A9EBB0539E1DA9A013E12499B5CEC3
Malicious:	false
Preview:	SQLite format 3.....@ .....K.....g....8..... ....

C:\ProgramData\59242670612831660624168672

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3034000, page size 2048, file counter 6, database pages 53, cookie 0x22, schema 4, UTF-8, version-valid-for 6
Category:	dropped
Size (bytes):	110592
Entropy (8bit):	1.103154063201814
Encrypted:	false
SSDEEP:	192:GLKnLLJFXH92HbG9mTjwnWxDnP1r6TVum:CKXJF392OnsDnRyVum
MD5:	A7888E78317DB24AF1E57A1E76360A05
SHA1:	350BC0A9A062F2290D8E41D17CACE4B49833918C
SHA-256:	34553CD7235802E2D02A4B1614D4C468E220377771CC7CB1A3F4D89580158534
SHA-512:	B705C5B67A2B294EB2951D19863F1FA729CE560C00378509D52AFDCBFAB824D754E32B013AB1318C17E9BC66B584471BFC01362A2BD3002AB3C388336ECD03EA
Malicious:	false
Preview:	SQLite format 3.....@ .....5....."....K.....*..... ....

C:\ProgramData\60379239670748708072323449

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3041002, page size 2048, file counter 7, database pages 57, cookie 0x30, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	1.202433056168029
Encrypted:	false
SSDEEP:	192:8mEcY8dBLH95TkVb39nJnieheVuKht6jTAs5u:8JcYiBz9EJnieheVuK7u0s8
MD5:	1D1D49B9691A566CD1923A0929480A3D
SHA1:	93976FCE24A3C1F8ECED9E2516BD775215AA5834
SHA-256:	FE23175F9F3E20359907D9A10FC3A7210F4D60096EA38A1AD2CBC86AAE015ABC
SHA-512:	3B6B31D164CB51C9B6740D82BEA21EB66E30B7E7AF0672B0AB1A7C860FB9FA81D7FFC651BE93BDD5AC76AE4191C6C3402F835F8D6FA807ECF005EA5CE6A856D3
Malicious:	false
Preview:	SQLite format 3.....@ .....9.....0.....f.....6..... ....

C:\ProgramData\77364074545019038892817732

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, user version 74, last written using SQLite version 3041002, page size 32768, writer version 2, read version 2, file counter 3, database pages 52, 1st free page 43, free pages 8, cookie 0x3c, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	5242880
Entropy (8bit):	0.039925776426730376
Encrypted:	false
SSDEEP:	192:itgVHwkYjcoBMc54tp9JWGDhIP5zZR38S3Z75pFh0:itgVHwVTBMc5lkG9Wf3z3Z75
MD5:	B9ABE44D5E5C8FF32C4A4F7C00354D61
SHA1:	585A3DD6093C2CE42305D39246CE8AF5508C4CC0
SHA-256:	F653A7A2AEF36FA73325DAB81A55D6118DF33713846E3931B5440FCF366686F6
SHA-512:	1F65EB719242A94E00D829D93B69B0874933BFD8C7B90053558A1187A3B7099B89E7F973E84177718BC03AD9E7DD2FB9B91F118A5E27B2BBBB990FD66315FA0E
Malicious:	false

Preview:	SQLite format 3.....@ .....4...+.....<.....J.....f..[R.+Yq.d@..a.|.|>{.{cz.zky.Yqx.x.w.v.wJu't>t.s.sLr.r:q.p.q|p.o.o.o.m.mQl.kok.g.g#f.egf!Z. Zya]ZyZyZyZyZyZyZy.....

C:\ProgramData\77364074545019038892817732-shm

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.017262956703125623
Encrypted:	false
SSDEEP:	3:G8lQs2TSlElQs2TtPRp//:G0QjSaQjrpX
MD5:	B7C14EC6110FA820CA6B65F5AEC85911
SHA1:	608EEB7488042453C9CA40F7E1398FC1A270F3F4
SHA-256:	FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB
SHA-512:	D8D75760F29B1E27AC9430BC4F4FFCEC39F1590BE5AEF2BFB5A535850302E067C288EF59CF3B2C5751009A22A6957733F9F80FA18F2B0D33D90C068A3F08F3B
Malicious:	false
Preview:	..-.....8...5.....-.....8...5.....

C:\ProgramData\93702365600485792059963927

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3034000, file counter 5, database pages 29, cookie 0x16, schema 4, UTF-8, version-valid-for 5
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.8330799750773747
Encrypted:	false
SSDEEP:	192:5A6DwbHq260V37/+bDo3irhnydVj3XBBE3uEUM:5AvHMi37wU3iVy/BBE3ulM
MD5:	5B8792E38274088A888A41F4AE3709EB
SHA1:	102DCDBAF4DDB1E3E37859EC1EDD1C788D75AF11
SHA-256:	090F856C8BD32598418336550AE669A11D44B9498FD7DDA794460D8B08F55515
SHA-512:	5B57092076CAFDECE39018B47DC6899F4D4F53E3EFD710AB471B00E0DE477E26868145C389E6841A5AC7840F9968FABF97AA5459520F51C6EA36EC71C8E089C 5
Malicious:	false
Preview:	SQLite format 3.....@ .....K.....

C:\ProgramData\98279768849475661070206458

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3041002, file counter 14, database pages 22, 1st free page 6, free pages 8, cookie 0x8, schema 4, UTF-8, version-valid-for 14
Category:	dropped
Size (bytes):	90112
Entropy (8bit):	3.5602851208577553
Encrypted:	false
SSDEEP:	768:Tanu5W7bpb5dOkhZM0a0SY+Oqa2XZvMYqVc:4u5W7ZXP3a0SY+Od2J0YOc
MD5:	B04B4FB2B7BD981A8698F42E5EA48FDE
SHA1:	5BE8B2A3F95D8B87726465937FBACD576443FA83
SHA-256:	D9D557C4E05A16DA0AFC2BDA66610256BA39A75746958FFF5F4A10DBC028ABC3
SHA-512:	03D7B867743C5142A164C47482863E7AFB1E4636A15476D175C3F7003D504EDEFAAB3687E47A0C8B052E233966CC6779F7B4B5C530B02DABF24399E86A59CEE
Malicious:	false
Preview:	SQLite format 3.....@ .....f.....f..g...f.....

C:\ProgramData\freebl3.dll

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	685392
Entropy (8bit):	6.872871740790978
Encrypted:	false
SSDEEP:	12288:4gPbPpxMofhPNN0+RXBrp3M5pzRN4l2SQ+PEu9tUs/abAQb51FW/IzkOfWPO9UN7:4gPbPp9NNP0BgInfW2WMC4M+hW
MD5:	550686C0EE48C386DFCB40199BD076AC
SHA1:	EE5134DA4D3EFCB466081FB6197BE5E12A5B22AB
SHA-256:	EDD043F2005DBD5902FC421EABB9472A7266950C5CBACA34E2D590B17D12F5FA
SHA-512:	0B7F47AF883B99F9FBDC08020446B58F2F3FA55292FD9BC78FC967DD35BDD8BD549802722DE37668CC89EDE61B20359190EFBFDF026AE2BDC854F4740A5464E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....4.....p.....@A....H...S.....x.....F..P/.....#..... .....@.....text..... ..`.rdata..... .....@..@.data...<F..0.....@....00cfg.....@..@.rsrc...x.....@..@.reloc...#.....$..."..... .....@..B.....

C:\ProgramData\mozglue.dll

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	608080
Entropy (8bit):	6.833616094889818
Encrypted:	false
SSDEEP:	12288:BlSyAom/gcRKMdRm4wFkRHuyG4RRGJVDjMk/x21R8gY/r:BKgcRKMdRm4wFkVVDGJVv//x21R8br
MD5:	C8FD9BE83BC728CC04BEFFAFC2907FE9
SHA1:	95AB9F701E0024CEDFBD312BCFE4E726744C4F2E
SHA-256:	BA06A6EE0B15F5BE5C4E67782EEC8B521E36C107A329093EC400FE0404EB196A
SHA-512:	FBB446F4A27EF510E616CAAD52945D6C9CC1FD063812C41947E579EC2B54DF57C6DC46237DED80FCA5847F38CBE1747A6C66A13E2C8C19C664A72BE35EB8B40
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....^.....j.....@A....`...W.....P/...0...A...S.....h.....Z.....text...a..... ..`.rdata.....@..@.data...D.....@....00cfg.....@..@.tls.....@....rsrc..... .....@..@.reloc...A...0...B.....@..B.....

C:\ProgramData\msvcp140.dll

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	450024
Entropy (8bit):	6.673992339875127
Encrypted:	false
SSDEEP:	12288:McPa9C9VbL+3Omy5CvyOvzeOKdqhUgiW6QR7t5s03Ooc8dHkC2esGAWf:McPa90Vbky5CvyUeOKn03Ooc8dHkC2eN
MD5:	5FF1FCA37C466D6723EC67BE93B51442
SHA1:	34CC4E158092083B13D67D6D2BC9E57B798A303B
SHA-256:	5136A49A682AC8D7F1CE71B211DE8688FCE42ED57210AF087A8E2DBC8A934062
SHA-512:	4802EF62630C521D83A1D333969593FB00C9B38F82B4D07F70FBD21F495FEA9B3F67676064573D2C71C42BC6F701992989742213501B16087BB6110E337C7546
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1C.._..._..._)n..._....._...^."._..^..._..\..._..[..._..Z..._..._..._..._..]..._.Rich.._.....PE..L.....0]....."!....(.....`.....@.....,....@A.....g.....r.....A.....=..`x..8.....w..@.....p.....c..@.....text....&.....(..... ..`.data...H)...@.....,.....@....idata.....p.....D.....@..@.didat..4.....X.....@....rsrc.....Z.....@..@.reloc...=.....>..^.....@..B.....

C:\ProgramData\nss3.dll

Process:	C:\Users\user\Desktop\file.exe

File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2046288
Entropy (8bit):	6.787733948558952
Encrypted:	false
SSDEEP:	49152:fECf12gikHlnKGxJRIB+y5nvxnaOSJ3HFNWYrVvE4CQsgzMmQfTU1NrWmy4KoAzh:J7Tf8J1Q+SS5/nr
MD5:	1CC453CDF74F31E4D913FF9C10ACDDE2
SHA1:	6E85EAE544D6E965F15FA5C39700FA7202F3AAFE
SHA-256:	AC5C92FE6C51CFA742E475215B83B3E11A4379820043263BF50D4068686C6FA5
SHA-512:	DD9FF4E06B00DC831439BAB11C10E9B2AE864EA6E780D3835EA7468818F35439F352EF137DA111EFCDF2BB6465F6CA486719451BF6CF32C6A4420A56B1D6457 1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....`.....p.....l- ...@A.... .....&.....@....P..x.....P/...`..\.....\....&..@.....text..... ..`.rdata..l.....@..@.data...DR.. .....@....00cfg.....@.....@..@.rsrc...x....P.....@..@.reloc..\....`.....@..B.....

C:\ProgramData\softokn3.dll

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	257872
Entropy (8bit):	6.727482641240852
Encrypted:	false
SSDEEP:	6144:/yF/zX2zfRkU62THVh/T2AhZxv6A31obD6Hq/8jis+FvtVRpsAAs0o8OqTYz+xnU:/yRzX2zfRkX2T1h/SA5PF9m8jJqKYz+y
MD5:	4E52D739C324DB8225BD9AB2695F262F
SHA1:	71C3DA43DC5A0D2A1941E874A6D015A071783889
SHA-256:	74EBBAC956E519E16923ABDC5AB8912098A4F64E38DDCB2EAE23969F306AFE5A
SHA-512:	2D4168A69082A9192B9248F7331BD806C260478FF817567DF54F997D7C3C7D640776131355401E4BDB9744E246C36D658CB24B18DE67D8F23F10066E5FE445F6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....4.c....."!.....P.....Sg ....@A.....Dv..S....w.....P/.....5..8q.....{.....text...&..... ..`.rdata.....@..@.da ta.....|.....@....00cfg.....@..@.rsrc.....@..@.reloc...5.....6.....@..B.....

C:\ProgramData\vcruntime140.dll

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	80880
Entropy (8bit):	6.920480786566406
Encrypted:	false
SSDEEP:	1536:lw2886xv555et/MCsjw0BuRK3jteo3ecbA2W86b+Ld:lw28V55At/zqw+lq9ecbA2W8H
MD5:	A37EE36B536409056A86F50E67777DD7
SHA1:	1CAFA159292AA736FC595FC04E16325B27CD6750
SHA-256:	8934AAEB65B6E6D253DFE72DEA5D65856BD871E989D5D3A2A35EDFE867BB4825
SHA-512:	3A7C260646315CF8C01F44B2EC60974017496BD0D80DD055C7E43B707CADBA2D63AAB5E0EFD435670AA77886ED86368390D42C4017FC433C3C4B9D1C47D0F3 6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....08e.....u.....Rich..... .....PE..L...|.0].....!.....0.....m....@A.....A... ....8..... ..@..... .....text..... ..`.data.....@....idata.....@..@.rsrc.....@..@.reloc..... .....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.835147897989796
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	file.exe
File size:	467'456 bytes
MD5:	bf81661814944b92da689f1c461ef908
SHA1:	7e3235d7ce69217063f53840e6337633cc721ec7
SHA256:	a524fce6eb4ee25ed07de294220d9c2445090b6c18b48802219149162152fea1
SHA512:	0cd9c1bc55c398240c8f7214d2928684de8ddc84d208327f5ec1905956421eaf63a2c8a98223a6e8d57780d57f13698162c1e7cc7cc54f76a8bf0a3870b2aa6a
SSDEEP:	6144:WWcIRLTO5mqX94gHnlqzeI+Dv73D7yAACFNs3/Aw/OzcGzVN:0IRLTRC94gH8zeTb7T7yNCrs3IzzcU
TLSH:	66A49D0352A1BC61E5264B729F1FC6F8BA1DF570BD897B663318AA6F04B01B3C663741
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....]typ...#...#...#.G.#...#.G.#/..#.G.#...#>.l#...#...#d..#.G.#...#.G.#...#.G.#...#Rich...#.....PE..L....t.b...

File Icon

Icon Hash:	5145494905514509

Static PE Info

General

Entrypoint:	0x4086fc
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x62C474C5 [Tue Jul 5 17:28:37 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	2f69518aa1d8a1d2ce824b07104b5c0f

Entrypoint Preview

Instruction
call 00007F3728BD1041h
jmp 00007F3728BC965Dh
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
xor ecx, ecx
cmp eax, dword ptr [0044E0F8h+ecx*8]
je 00007F3728BC97F5h
inc ecx
cmp ecx, 2Dh
jc 00007F3728BC97D3h
lea ecx, dword ptr [eax-13h]
cmp ecx, 11h

Instruction
jnbe 00007F3728BC97F0h
push 0000000Dh
pop eax
pop ebp
ret
mov eax, dword ptr [0044E0FCh+ecx*8]
pop ebp
ret
add eax, FFFFFF44h
push 0000000Eh
pop ecx
cmp ecx, eax
sbb eax, eax
and eax, ecx
add eax, 08h
pop ebp
ret
call 00007F3728BCE8C5h
test eax, eax
jne 00007F3728BC97E8h
mov eax, 0044E260h
ret
add eax, 08h
ret
call 00007F3728BCE8B2h
test eax, eax
jne 00007F3728BC97E8h
mov eax, 0044E264h
ret
add eax, 0Ch
ret
mov edi, edi
push ebp
mov ebp, esp
push esi
call 00007F3728BC97C7h
mov ecx, dword ptr [ebp+08h]
push ecx
mov dword ptr [eax], ecx
call 00007F3728BC9767h
pop ecx
mov esi, eax
call 00007F3728BC97A1h
mov dword ptr [eax], esi
pop esi
pop ebp
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 4Ch
mov eax, dword ptr [0044E270h]
xor eax, ebp
mov dword ptr [ebp-04h], eax
push ebx
xor ebx, ebx
push esi
mov esi, dword ptr [ebp+08h]
push edi

Instruction
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-1Ch], ebx
mov dword ptr [ebp-20h], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-24h], ebx
mov dword ptr [ebp-4Ch], esi
mov dword ptr [ebp-48h], ebx
cmp dword ptr [esi+14h], ebx

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C++] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4d52c	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x203d000	0x17958	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2055000	0x1394	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1220	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x3bf8	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1c0	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x4cf90	0x4d000	False	0.8349419135551948	data	7.723744016228705	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x4e000	0x1fee8c4	0x2200	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x203d000	0x17958	0x17a00	False	0.36691881613756616	data	4.176871845508122	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2055000	0xb034	0xb200	False	0.0936402738764045	data	1.1823194980378087	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
AFX_DIALOG_LAYOUT	0x20521d8	0xe	data	Punjabi	Pakistan	1.5714285714285714
AFX_DIALOG_LAYOUT	0x20521d8	0xe	data	Punjabi	India	1.5714285714285714
AFX_DIALOG_LAYOUT	0x20521e8	0xe	data	Punjabi	Pakistan	1.5714285714285714
AFX_DIALOG_LAYOUT	0x20521e8	0xe	data	Punjabi	India	1.5714285714285714
RT_CURSOR	0x20521f8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Punjabi	Pakistan	0.27238805970149255
RT_CURSOR	0x20521f8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Punjabi	India	0.27238805970149255

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_CURSOR	0x20530a0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Punjabi	Pakistan	0.375
RT_CURSOR	0x20530a0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Punjabi	India	0.375
RT_CURSOR	0x2053948	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Punjabi	Pakistan	0.5057803468208093
RT_CURSOR	0x2053948	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Punjabi	India	0.5057803468208093
RT_ICON	0x203d7a0	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Punjabi	Pakistan	0.35767590618336886
RT_ICON	0x203d7a0	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Punjabi	India	0.35767590618336886
RT_ICON	0x203e648	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Punjabi	Pakistan	0.4760830324909747
RT_ICON	0x203e648	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Punjabi	India	0.4760830324909747
RT_ICON	0x203eef0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Punjabi	Pakistan	0.4645228215767635
RT_ICON	0x203eef0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Punjabi	India	0.4645228215767635
RT_ICON	0x2041498	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Punjabi	Pakistan	0.4704502814258912
RT_ICON	0x2041498	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Punjabi	India	0.4704502814258912
RT_ICON	0x2042540	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Punjabi	Pakistan	0.49645390070921985
RT_ICON	0x2042540	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Punjabi	India	0.49645390070921985
RT_ICON	0x20429f8	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Punjabi	Pakistan	0.41647465437788017
RT_ICON	0x20429f8	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Punjabi	India	0.41647465437788017
RT_ICON	0x20430c0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Punjabi	Pakistan	0.26441908713692946
RT_ICON	0x20430c0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Punjabi	India	0.26441908713692946
RT_ICON	0x2045668	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Punjabi	Pakistan	0.324468085106383
RT_ICON	0x2045668	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Punjabi	India	0.324468085106383
RT_ICON	0x2045b00	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Punjabi	Pakistan	0.37100213219616207
RT_ICON	0x2045b00	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Punjabi	India	0.37100213219616207
RT_ICON	0x20469a8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Punjabi	Pakistan	0.45306859205776173
RT_ICON	0x20469a8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Punjabi	India	0.45306859205776173
RT_ICON	0x2047250	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Punjabi	Pakistan	0.4539170506912442
RT_ICON	0x2047250	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Punjabi	India	0.4539170506912442
RT_ICON	0x2047918	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Punjabi	Pakistan	0.4515895953757225
RT_ICON	0x2047918	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Punjabi	India	0.4515895953757225
RT_ICON	0x2047e80	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Punjabi	Pakistan	0.26950207468879667
RT_ICON	0x2047e80	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Punjabi	India	0.26950207468879667
RT_ICON	0x204a428	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Punjabi	Pakistan	0.3058161350844278
RT_ICON	0x204a428	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Punjabi	India	0.3058161350844278
RT_ICON	0x204b4d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Punjabi	Pakistan	0.3617021276595745
RT_ICON	0x204b4d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Punjabi	India	0.3617021276595745
RT_ICON	0x204b9a0	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Punjabi	Pakistan	0.5191897654584222

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0x204b9a0	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Punjabi	India	0.5191897654584222
RT_ICON	0x204c848	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Punjabi	Pakistan	0.5085740072202166
RT_ICON	0x204c848	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Punjabi	India	0.5085740072202166
RT_ICON	0x204d0f0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Punjabi	Pakistan	0.45622119815668205
RT_ICON	0x204d0f0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Punjabi	India	0.45622119815668205
RT_ICON	0x204d7b8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Punjabi	Pakistan	0.4761560693641618
RT_ICON	0x204d7b8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Punjabi	India	0.4761560693641618
RT_ICON	0x204dd20	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	Punjabi	Pakistan	0.28143153526970954
RT_ICON	0x204dd20	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	Punjabi	India	0.28143153526970954
RT_ICON	0x20502c8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	Punjabi	Pakistan	0.30816135084427765
RT_ICON	0x20502c8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	Punjabi	India	0.30816135084427765
RT_ICON	0x2051370	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	Punjabi	Pakistan	0.3368852459016393
RT_ICON	0x2051370	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	Punjabi	India	0.3368852459016393
RT_ICON	0x2051cf8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	Punjabi	Pakistan	0.375
RT_ICON	0x2051cf8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	Punjabi	India	0.375
RT_STRING	0x2054150	0xb8	data	Punjabi	Pakistan	0.5815217391304348
RT_STRING	0x2054150	0xb8	data	Punjabi	India	0.5815217391304348
RT_STRING	0x2054208	0x74a	data	Punjabi	Pakistan	0.42497320471597
RT_STRING	0x2054208	0x74a	data	Punjabi	India	0.42497320471597
RT_GROUP_CURSOR	0x2053eb0	0x30	data	Punjabi	Pakistan	0.9375
RT_GROUP_CURSOR	0x2053eb0	0x30	data	Punjabi	India	0.9375
RT_GROUP_ICON	0x20429a8	0x4c	data	Punjabi	Pakistan	0.75
RT_GROUP_ICON	0x20429a8	0x4c	data	Punjabi	India	0.75
RT_GROUP_ICON	0x204b938	0x68	data	Punjabi	Pakistan	0.7115384615384616
RT_GROUP_ICON	0x204b938	0x68	data	Punjabi	India	0.7115384615384616
RT_GROUP_ICON	0x2045ad0	0x30	data	Punjabi	Pakistan	0.9791666666666666
RT_GROUP_ICON	0x2045ad0	0x30	data	Punjabi	India	0.9791666666666666
RT_GROUP_ICON	0x2052160	0x76	data	Punjabi	Pakistan	0.6694915254237288
RT_GROUP_ICON	0x2052160	0x76	data	Punjabi	India	0.6694915254237288
RT_VERSION	0x2053ee0	0x270	data	Punjabi	Pakistan	0.5272435897435898
RT_VERSION	0x2053ee0	0x270	data	Punjabi	India	0.5272435897435898

Imports

DLL	Import

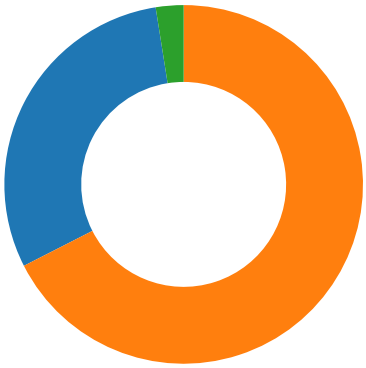
DLL	Import
KERNEL32.dll	GetDateFormatW, UnregisterWait, FindResourceA, FindFirstFileW, FindFirstChangeNotificationW, SetFilePointer, GetConsoleAliasesLengthW, PeekNamedPipe, SetComputerNameExA, GetCurrentProcess, SetEnvironmentVariableW, InterlockedCompareExchange, AddConsoleAliasW, CreateHardLinkA, FreeEnvironmentStringsA, GetModuleHandleW, ReadConsoleInputA, CopyFileW, GetSystemWindowsDirectoryA, GetConsoleAliasExesLengthW, CreateFileW, GetVolumePathNameA, GetLastError, SetLastError, ReadConsoleOutputCharacterA, GetProcAddress, VirtualAlloc, VirtualAllocEx, SetFileApisToOEM, LoadLibraryA, InterlockedExchangeAdd, BuildCommDCBAndTimeoutsW, FindAtomA, GetOEMCP, GetModuleHandleA, FreeEnvironmentStringsW, EnumResourceNamesA, GetConsoleTitleW, GetShortPathNameW, FileTimeToLocalFileTime, FindFirstVolumeW, QueryDepthSList, FindNextVolumeA, AreFileApisANSI, CreateFileA, CloseHandle, WideCharToMultiByte, InterlockedIncrement, InterlockedDecrement, InterlockedExchange, MultiByteToWideChar, Sleep, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, HeapFree, TerminateProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetCommandLineA, GetStartupInfoA, GetCPInfo, RtlUnwind, RaiseException, LCMapStringW, LCMapStringA, GetStringTypeW, HeapAlloc, HeapCreate, VirtualFree, HeapReAlloc, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, GetCurrentThreadId, HeapSize, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, GetEnvironmentStrings, GetEnvironmentStringsW, SetHandleCount, GetFileType, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, GetStringTypeA, GetACP, IsValidCodePage, GetUserDefaultLCID, GetLocaleInfoA, EnumSystemLocalesA, IsValidLocale, InitializeCriticalSectionAndSpinCount, SetStdHandle, GetConsoleCP, GetConsoleMode, FlushFileBuffers, GetLocaleInfoW, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW
USER32.dll	ChangeMenuA, LoadMenuW, GetMessageExtraInfo

Possible Origin

Language of compilation system	Country where language is spoken	Map
Punjabi	Pakistan	
Punjabi	India	

Network Behavior

Network Port Distribution



Total Packets: 40

- 53 (DNS)
- 6012 undefined
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2023 16:50:48.348377943 CEST	49773	443	192.168.2.8	149.154.167.99
Aug 31, 2023 16:50:48.348463058 CEST	443	49773	149.154.167.99	192.168.2.8
Aug 31, 2023 16:50:48.348647118 CEST	49773	443	192.168.2.8	149.154.167.99
Aug 31, 2023 16:50:48.372037888 CEST	49773	443	192.168.2.8	149.154.167.99
Aug 31, 2023 16:50:48.372093916 CEST	443	49773	149.154.167.99	192.168.2.8
Aug 31, 2023 16:50:48.448729038 CEST	443	49773	149.154.167.99	192.168.2.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2023 16:50:48.449021101 CEST	49773	443	192.168.2.8	149.154.167.99
Aug 31, 2023 16:50:48.699378967 CEST	49773	443	192.168.2.8	149.154.167.99
Aug 31, 2023 16:50:48.699475050 CEST	443	49773	149.154.167.99	192.168.2.8
Aug 31, 2023 16:50:48.700390100 CEST	443	49773	149.154.167.99	192.168.2.8
Aug 31, 2023 16:50:48.700628996 CEST	49773	443	192.168.2.8	149.154.167.99
Aug 31, 2023 16:50:48.704653025 CEST	49773	443	192.168.2.8	149.154.167.99
Aug 31, 2023 16:50:48.747484922 CEST	443	49773	149.154.167.99	192.168.2.8
Aug 31, 2023 16:50:48.748595953 CEST	443	49773	149.154.167.99	192.168.2.8
Aug 31, 2023 16:50:48.748656034 CEST	443	49773	149.154.167.99	192.168.2.8
Aug 31, 2023 16:50:48.748754978 CEST	49773	443	192.168.2.8	149.154.167.99
Aug 31, 2023 16:50:48.748779058 CEST	443	49773	149.154.167.99	192.168.2.8
Aug 31, 2023 16:50:48.748856068 CEST	443	49773	149.154.167.99	192.168.2.8
Aug 31, 2023 16:50:48.748857975 CEST	49773	443	192.168.2.8	149.154.167.99
Aug 31, 2023 16:50:48.748872042 CEST	49773	443	192.168.2.8	149.154.167.99
Aug 31, 2023 16:50:48.748925924 CEST	49773	443	192.168.2.8	149.154.167.99
Aug 31, 2023 16:50:48.752507925 CEST	49773	443	192.168.2.8	149.154.167.99
Aug 31, 2023 16:50:48.752535105 CEST	443	49773	149.154.167.99	192.168.2.8
Aug 31, 2023 16:50:48.757543087 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:48.779143095 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:48.779371023 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:48.779787064 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:48.800959110 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.066073895 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.066252947 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.400916100 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.422157049 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.422274113 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.422308922 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.422339916 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.422370911 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.422414064 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.422452927 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.422471046 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.422485113 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.422518969 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.422523022 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.422544003 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.422554016 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.422576904 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.422584057 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.422657013 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.443973064 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444034100 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444082022 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444128990 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444194078 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444241047 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444288969 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444324970 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.444336891 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444365025 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.444386959 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444431067 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.444437027 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444479942 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.444484949 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444531918 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.444531918 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444582939 CEST	6012	49774	195.201.254.123	192.168.2.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2023 16:50:49.444617987 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.444631100 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444658995 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.444709063 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444736004 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.444755077 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444791079 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.444803953 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444849014 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.444850922 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444897890 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444900990 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.444947958 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.444983959 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.445024967 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.445081949 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.466572046 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.466633081 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.466682911 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.466728926 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.466777086 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.466825008 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.466872931 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.466921091 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.466967106 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.467015028 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.467061043 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.467091084 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.467108011 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.467154980 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.467164040 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.467202902 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.467252970 CEST	6012	49774	195.201.254.123	192.168.2.8
Aug 31, 2023 16:50:49.467262030 CEST	49774	6012	192.168.2.8	195.201.254.123
Aug 31, 2023 16:50:49.467299938 CEST	6012	49774	195.201.254.123	192.168.2.8

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2023 16:50:48.321386099 CEST	52799	53	192.168.2.8	8.8.8.8
Aug 31, 2023 16:50:48.336807013 CEST	53	52799	8.8.8.8	192.168.2.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Aug 31, 2023 16:50:48.321386099 CEST	192.168.2.8	8.8.8.8	0x810	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Aug 31, 2023 16:50:48.336807013 CEST	8.8.8.8	192.168.2.8	0x810	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- t.me
- 195.201.254.123:6012

Statistics

No statistics

System Behavior

Analysis Process: file.exe PID: 7912, Parent PID: 4884

General

Target ID:	1
Start time:	16:50:20
Start date:	31/08/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	467'456 bytes
MD5 hash:	BF81661814944B92DA689F1C461EF908
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000002.3698889782.0000000004100000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000001.00000002.3698889782.0000000004100000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.3696575131.000000000252E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000001.00000002.3698810477.0000000004090000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000002.3693314502.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000003.1481373645.0000000004160000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low
Has exited:	false

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\vcruntime140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40A258	CreateFileA
C:\ProgramData\softokn3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40A258	CreateFileA
C:\ProgramData\nss3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40A258	CreateFileA
C:\ProgramData\msvcp140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40A258	CreateFileA
C:\ProgramData\mozglue.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40A258	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\freebl3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40A258	CreateFileA
C:\ProgramData\22428703343438507335441715	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	41630D	CopyFileA
C:\ProgramData\22428703343438507335441715-wal	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	61E49483	CreateFileW
C:\ProgramData\22428703343438507335441715-shm	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	61E49483	CreateFileW
C:\ProgramData\77364074545019038892817732	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	41668D	CopyFileA
C:\ProgramData\77364074545019038892817732-wal	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	61E49483	CreateFileW
C:\ProgramData\77364074545019038892817732-shm	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	61E49483	CreateFileW
C:\ProgramData\98279768849475661070206458	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	41B13E	CopyFileA
C:\ProgramData\05817041688375942296226764	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	415CBD	CopyFileA
C:\ProgramData\30562671907380543272507388	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	415E7D	CopyFileA
C:\ProgramData\41854390081158473842695081	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	41AD14	CopyFileA
C:\ProgramData\37707990510604932654966133	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	41B577	CopyFileA
C:\ProgramData\60379239670748708072323449	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	415ADD	CopyFileA
C:\ProgramData\52766014303501464703169876	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	41B13E	CopyFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\93702365600485792059963927	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	415CBD	CopyFileA
C:\ProgramData\38345013959471306846242542	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	415E7D	CopyFileA
C:\ProgramData\35746121865178509047716708	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	41AD14	CopyFileA
C:\ProgramData\59242670612831660624168672	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	41B577	CopyFileA
C:\ProgramData\00440746450577075373182215	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	415ADD	CopyFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\22428703343438507335441715-shm	success or wait	1	61E345D4	DeleteFileW
C:\ProgramData\22428703343438507335441715-wal	success or wait	1	61E345D4	DeleteFileW
C:\ProgramData\2242870334343850733544171 5	success or wait	1	4165FD	DeleteFileA
C:\ProgramData\77364074545019038892817732-shm	success or wait	1	61E345D4	DeleteFileW
C:\ProgramData\77364074545019038892817732-wal	success or wait	1	61E345D4	DeleteFileW
C:\ProgramData\7736407454501903889 2817732	success or wait	1	4167AA	DeleteFileA
C:\ProgramData\05817041688375942296226764	success or wait	1	415DE9	DeleteFileA
C:\ProgramData\30562671907380543272507388	success or wait	1	415FC1	DeleteFileA
C:\ProgramData\41854390081158473842695081	success or wait	1	41B029	DeleteFileA
C:\ProgramData\37707990510604932654966133	success or wait	1	41B7BE	DeleteFileA
C:\ProgramData\60379239670748708072323449	success or wait	1	415C20	DeleteFileA
C:\ProgramData\93702365600485792059963927	success or wait	1	415DE9	DeleteFileA
C:\ProgramData\38345013959471306846242542	success or wait	1	415FC1	DeleteFileA
C:\ProgramData\35746121865178509047716708	success or wait	1	41B029	DeleteFileA
C:\ProgramData\59242670612831660624168672	success or wait	1	41B7BE	DeleteFileA
C:\ProgramData\00440746450577075373182215	success or wait	1	415C20	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\ProgramData\vcruntime140.dll</td><td>0</td><td>16384</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd 44 fd fd fd fd fd fd fd fd fd fd 30 38 65 fd fd fd fd fd fd fd 19 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 09 fd fd fd fd fd fd 0e fd fd fd fd fd fd 0f fd fd fd fd fd fd 0a fd fd fd fd fd fd fd 75 fd fd fd fd fd fd 08 fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 7c fd 30 5d 00 00 00 00 00 00 00 00 fd 00 22</td><td>MZ@!L!This program cannot be run in DOS mode.$08euRichPEL|0]"</td><td>success or wait</td><td>5</td><td>40A337</td><td>WriteFile</td></tr>
<tr><td>C:\ProgramData\softokn3.dll</td><td>0</td><td>16384</td><td>4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 02 00 00 fd 00 00 00 00 00 00 50 fd 02 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 04 00 00 04 00 00 53 67 04 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 44 76 03 00 53 01 00 00 fd 77 03 00 fd 00 00</td><td>MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!PSg@A DvSw</td><td>success or wait</td><td>16</td><td>40A337</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\nss3.dll	0	16384	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 19 00 00 2e 05 00 00 00 00 00 60 fd 14 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 70 1f 00 00 04 00 00 6c 2d 20 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd 26 1d 00 fd fd 00 00 fd fd 1d 00 40 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!.`pl-@A&@	success or wait	125	40A337	WriteFile
C:\ProgramData\msvcp140.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 53 31 43 fd fd 5f 10 fd fd 5f 10 fd fd 5f 10 29 6e fd 10 fd fd 5f 10 fd fd fd 10 fd fd 5f 10 fd fd 5e 10 22 fd 5f 10 da 5e 11 fd fd 5f 10 da 5c 11 fd fd 5f 10 da 5b 11 fd fd 5f 10 da 5a 11 fd fd 5f 10 da 5f 11 fd fd 5f 10 da fd 10 fd fd 5f 10 da 5d 11 fd fd 5f 10 52 69 63 68 fd fd 5f 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$1C___)n__^"_^__[_Z____]_Rich_	success or wait	28	40A337	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\mozglue.dll	0	16384	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 07 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 07 00 00 5e 01 00 00 00 00 00 fd fd 03 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 09 00 00 04 00 00 6a fd 09 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 01 60 08 00 fd 57 00 00 fd 08 00 2c 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!^j@A`W,	success or wait	38	40A337	WriteFile
C:\ProgramData\freebl3.dll	0	16384	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd 34 12 63 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 0e 08 00 00 34 02 00 00 00 00 00 70 12 08 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 0a 00 00 04 00 00 fd fd 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 48 1c 0a 00 53 00 00 00 fd 1c 0a 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL4c"!4p@AHS	success or wait	42	40A337	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\22428703343438507335441715	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\22428703343438507335441715	0	32768	success or wait	2	61E33FB7	ReadFile
C:\ProgramData\22428703343438507335441715	32768	32768	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\77364074545019038892817732	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\77364074545019038892817732	0	32768	success or wait	2	61E33FB7	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	70296	success or wait	1	4157EA	ReadFile
C:\ProgramData\98279768849475661070206458	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\98279768849475661070206458	0	4096	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\05817041688375942296226764	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\05817041688375942296226764	0	4096	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\30562671907380543272507388	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\30562671907380543272507388	0	4096	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\41854390081158473842695081	0	100	success or wait	1	61E33FB7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\41854390081158473842695081	0	2048	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\37707990510604932654966133	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\37707990510604932654966133	0	2048	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\60379239670748708072323449	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\60379239670748708072323449	0	2048	success or wait	1	61E33FB7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	8756	success or wait	1	4157EA	ReadFile
C:\ProgramData\52766014303501464703169876	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\52766014303501464703169876	0	4096	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\93702365600485792059963927	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\93702365600485792059963927	0	4096	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\38345013959471306846242542	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\38345013959471306846242542	0	4096	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\35746121865178509047716708	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\35746121865178509047716708	0	2048	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\59242670612831660624168672	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\59242670612831660624168672	0	2048	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\00440746450577075373182215	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\00440746450577075373182215	0	2048	success or wait	1	61E33FB7	ReadFile

Disassembly

No disassembly